

ETSI TS 102 412 V11.2.0 (2019-06)



Smart Cards; Smart Card Platform Requirements Stage 1 (Release 11)

iTeh STANDARDS PREVIEW
(standards.iteh.ai)
Full standard: <https://standards.iteh.ai/catalog/standards/sls/8a7ec42d-5a66-412-b830-594889e8289b/etsi-ts-102-412-v11-2-0-2019-06>

ReferenceRTS/SCP-R00002vb20

Keywordssmart card

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2019.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M™ logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners.

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	9
Foreword.....	9
Modal verbs terminology.....	9
Introduction	10
1 Scope	11
2 References	11
2.1 Normative references	11
2.2 Informative references.....	12
3 Definition of terms, symbols and abbreviations.....	13
3.1 Terms.....	13
3.2 Symbols.....	15
3.3 Abbreviations	15
4 Requirements.....	17
4.0 General	17
4.1 Run time environment timing constraints	18
4.1.1 Abstract (informative).....	18
4.1.2 Background (informative).....	18
4.1.2.1 Use case - Network authentication.....	18
4.1.3 Requirements	19
4.1.4 Interaction with existing features (informative).....	19
4.2 Launch Application feature	19
4.2.1 Abstract (informative).....	19
4.2.2 Background (informative).....	19
4.2.3 Requirements	20
4.2.4 Interaction with existing features (informative).....	20
4.3 Mapped file support on the UICC	20
4.3.1 Abstract (informative).....	20
4.3.2 Background (informative).....	21
4.3.3 Requirements	21
4.3.4 Interaction with existing features (informative).....	21
4.4 Extension of logical channels.....	21
4.4.1 Abstract (informative).....	21
4.4.2 Background (informative).....	21
4.4.2.1 Typical problem situation	21
4.4.2.2 Possible problem solution	22
4.4.2.3 Use cases	22
4.4.2.3.1 Use case - JSR 177 applications	22
4.4.2.3.2 Use case - PC connection	22
4.4.3 Requirements	22
4.4.3.1 General requirements	22
4.4.3.2 Backward compatibility requirements.....	22
4.4.4 Interaction with existing features (informative).....	22
4.5 Secure channel to secure local terminal interfaces	22
4.5.1 Abstract (informative).....	22
4.5.2 Background (informative).....	23
4.5.2.0 General	23
4.5.2.1 Use case - User interface.....	23
4.5.2.2 Use case - UICC as a control point for device management.....	24
4.5.2.3 Use case - DRM and distributed applications	25
4.5.2.4 Use case - Toolkit commands protection	27
4.5.3 Requirements	27
4.5.3.0 General	27
4.5.3.1 End point requirements	27
4.5.3.2 Integrity requirements	27

4.5.3.3	Confidentiality requirements	28
4.5.3.4	Authentication requirements	28
4.5.3.5	Audit/Compliance requirements	28
4.5.3.6	Policy requirements	28
4.5.3.7	Transport Protocol requirements	28
4.5.4	Interaction with existing features (informative)	28
4.5.4.1	Logical Channels	28
4.6	Authenticate command longer than 255 bytes	28
4.6.1	Abstract (informative)	28
4.6.2	Background (informative)	29
4.6.2.1	Use case - EAP packet exchange	29
4.6.3	Requirements	29
4.6.3.1	General requirements	29
4.6.3.2	Backward compatibility requirements	29
4.6.4	Interaction with existing features (informative)	29
4.7	CAT mechanisms to indicate the bearer connection status	29
4.7.1	Abstract (informative)	29
4.7.2	Background (informative)	29
4.7.2.1	Use case - Availability of network bearers	29
4.7.2.2	Use case - Network connection temporarily lost	30
4.7.2.3	Use case - Availability of local bearers	30
4.7.3	Requirements	30
4.7.3.1	Requirement 1 - Network bearer connection status	30
4.7.3.2	Requirement 2 - Local bearer connection status	30
4.7.4	Interaction with existing features (informative)	30
4.8	New UICC-Terminal interface	30
4.8.1	Abstract (informative)	30
4.8.2	Background (informative)	31
4.8.2.0	General	31
4.8.2.1	Use case - multimedia file management	31
4.8.2.2	Use case - MMI on UICC	31
4.8.2.3	Use case - real-time multimedia data encryption/decryption	31
4.8.2.4	Use case - storage of terminal applications on the UICC	31
4.8.2.5	Use case - direct and indirect UICC connection to a PC	31
4.8.2.6	Use case - web server on Smart Card	32
4.8.2.7	Use case - antivirus on UICC	32
4.8.2.8	Use case - big phonebook management from the UICC	32
4.8.2.9	Use case - reduce personalization time	32
4.8.2.10	Use case - generic TCP/IP connectivity	32
4.8.3	Requirements	33
4.8.3.1	General requirements	33
4.8.3.2	Backward compatibility requirements	33
4.8.4	Interaction with existing features (informative)	34
4.9	UICC based application acting as a server	34
4.9.1	Abstract (informative)	34
4.9.2	Background (informative)	34
4.9.3	Requirements	34
4.9.4	Interaction with existing features (informative)	34
4.10	API for applications registered to a Smart Card Web Server	34
4.10.1	Abstract (informative)	34
4.10.2	Background (informative)	35
4.10.2.0	General	35
4.10.2.1	Registration of an application to the SCWS	35
4.10.2.2	Data exchange between SCWS and application	35
4.10.2.3	Issuing Proactive Commands	35
4.10.3	Requirements	35
4.10.4	Interaction with existing features (informative)	36
4.11	Specific UICC environmental conditions	36
4.11.1	Abstract (informative)	36
4.11.2	Background (informative)	36
4.11.2.0	General	36
4.11.2.1	Use case - Automotive service	36

4.11.2.2	Use case - Remote monitoring camera.....	36
4.11.2.3	Use case - Remote stock monitoring for vending machines	36
4.11.2.4	Use case - Online electronic advertising board	36
4.11.3	Considerations (informative)	36
4.11.4	Requirements	37
4.11.4.1	Requirement 1: Temperature range	37
4.11.4.2	Requirement 2: Humidity	37
4.11.5	Interaction with existing features (informative).....	37
4.12	Introduction of high density memory technology in UICC	37
4.12.1	Abstract (informative).....	37
4.12.2	Background (informative).....	37
4.12.2.1	Use case - Enhanced UICC features.....	37
4.12.3	Requirements	38
4.12.4	Interaction with existing features (informative).....	38
4.13	Power supply indication mechanism	38
4.13.1	Abstract (informative).....	38
4.13.2	Background (informative).....	38
4.13.2.1	Use case - generic situation	38
4.13.2.2	Use case - USIM application with toolkit applications	39
4.13.3	Requirements	39
4.13.3.1	General Requirements	39
4.13.3.2	Backward compatibility requirements.....	39
4.13.4	Interaction with existing features (informative).....	39
4.14	Internet Connectivity up to UICC applications	39
4.14.1	Abstract (informative).....	39
4.14.2	Use Cases (informative).....	40
4.14.2.0	General	40
4.14.2.1	Use Case - Card OTA management	40
4.14.2.2	Use Case - User local access from the terminal to a card server	40
4.14.2.3	Use Case - Remote access to an identity server in the card	41
4.14.2.4	Use Case - User access from a locally connected device to a card service	41
4.14.3	Requirements	41
4.14.4	Interaction with existing features (informative).....	41
4.15	Contactless UICC services	42
4.15.1	Abstract (informative).....	42
4.15.2	Background (informative).....	42
4.15.2.0	General	42
4.15.2.1	Use case - Access	42
4.15.2.1.1	System aspects of use case	42
4.15.2.1.2	UICC role in use case	43
4.15.2.2	Use case - tickets	44
4.15.2.2.0	General	44
4.15.2.2.1	System aspects of throughput ticketing scenario	44
4.15.2.2.2	System aspects of high priced ticketing scenario	44
4.15.2.2.3	UICC role in use case	45
4.15.2.3	Use case - digital rights	46
4.15.2.3.1	System aspects of contactless digital rights	46
4.15.2.3.2	UICC role in use case	46
4.15.2.4	Use case - payment application	47
4.15.2.5	Use case - loyalty application.....	47
4.15.2.6	Use case - health care application	48
4.15.2.7	Use case - retail	48
4.15.2.7.1	System aspects of the use case	48
4.15.2.7.2	UICC role in the use case	48
4.15.2.8	Consideration about multiple applications in peer to peer mode	49
4.15.2.8.1	System aspects of multiple applications in peer to peer mode	49
4.15.2.8.2	Service discovery in peer to peer mode	49
4.15.2.8.3	Application connection in peer to peer mode	49
4.15.2.8.4	Customer care in peer to peer mode	49
4.15.2.9	Considerations about the P2P technology	49
4.15.3	Requirements	50
4.15.3.1	Physical interface requirements	50

4.15.3.2	Multi-protocol concurrent operation requirements	50
4.15.3.3	Contactless communication modes requirements	50
4.15.3.4	Compatibility with existing contactless systems requirements	51
4.15.3.5	Parameters to be transported by the CLFIP requirements	51
4.15.3.6	Application integration requirements	51
4.15.3.7	Terminal and user interaction requirements	51
4.15.3.8	Interoperability requirements	51
4.15.3.9	RFID requirements	52
4.15.3.10	P2P mode requirements	52
4.15.3.10.1	General P2P requirements	52
4.15.3.10.2	P2P application management requirements	53
4.15.4	Interaction with existing features (informative)	54
4.16	Administration of the Smart Card Web Server	54
4.16.1	Abstract (informative)	54
4.16.2	Background (informative)	54
4.16.3	Requirements	54
4.16.4	Interaction with existing features (informative)	54
4.17	Confidential Application Services	54
4.17.1	Abstract (informative)	54
4.17.2	Background (informative)	55
4.17.2.1	Use case 1: Mobile TV services	55
4.17.2.2	Use case 2: Banking Services	56
4.17.2.3	Use case 3: Contactless Applications	57
4.17.2.4	Use case 4: Mobile Virtual Network Operator services	58
4.17.3	Requirements (normative)	59
4.17.3.0	General	59
4.17.3.1	Confidential application environment	59
4.17.3.2	Administration by Card issuer	59
4.17.3.2.1	Third party area environment administration	59
4.17.3.2.2	Third party area creation	60
4.17.3.2.3	Third party area policy definition	60
4.17.3.3	Administration by Third party	60
4.17.3.4	Service Operator specific requirements	61
4.17.4	Interaction with existing features (informative)	61
4.18	UICC for Machine-to-Machine (M2M) applications	61
4.18.1	Abstract (informative)	61
4.18.2	Use Cases (informative)	62
4.18.2.1	Use case - Track and Trace	62
4.18.2.1.0	General	62
4.18.2.1.1	Use case - Emergency Call	62
4.18.2.1.2	Use case - Fleet Management	63
4.18.2.1.3	Use case - Theft Tracking	63
4.18.2.2	Use case - Monitoring	64
4.18.2.2.0	General	64
4.18.2.2.1	Use case - Metering/Prepaid delivery of utilities (water, gas, electricity)	64
4.18.2.2.2	Use case - Person / Animal protection	65
4.18.2.2.3	Use case - Object protection	65
4.18.2.3	Use case - Transaction	66
4.18.2.3.1	Use case - PoS Terminals (Point of Sale Terminals)	66
4.18.2.4	Use case - Control	66
4.18.2.4.1	Use case - Controlling vending machines	66
4.18.2.4.2	Use case - Controlling production machines	67
4.18.3	Requirements	67
4.18.3.0	General	67
4.18.3.1	General M2M UICC Requirements	67
4.18.3.1.0	General	67
4.18.3.1.1	Specific requirements related to definition of classes	68
4.18.3.1.2	Example for a possible class system (informative)	68
4.18.3.2	MFF Requirements	68
4.18.4	Interaction with existing features (informative)	69
4.19	Location based services for broadcast technology	69
4.19.1	Abstract (informative)	69

4.19.2	Use Cases (informative).....	69
4.19.3	Requirement for retrieving location information for broadcast technology.....	69
4.19.4	Interaction with existing features (informative).....	69
4.20	Terminals with reduced functionality.....	69
4.20.1	Abstract (informative).....	69
4.20.2	Use case (informative).....	70
4.20.2.1	Use case - Data card.....	70
4.20.3	Requirements.....	70
4.20.4	Interaction with existing features (informative).....	70
4.21	Digital Rights Management.....	70
4.21.1	Abstract (informative).....	70
4.21.2	Use cases (informative).....	70
4.21.2.0	General.....	70
4.21.2.1	Use case - Transfer of protected contents and rights by using a UICC.....	70
4.21.2.2	Use case - Provisioning of rights in the UICC.....	71
4.21.2.3	Use case - Direct rendering of DRM-protected content by using the UICC.....	71
4.21.2.4	Use case - Pre-loading of rights by using the UICC.....	71
4.21.3	Requirements.....	71
4.21.4	Interaction with existing features (informative).....	71
4.22	Multicast dataflow in UICC.....	72
4.22.1	Abstract (informative).....	72
4.22.2	Use cases (informative).....	72
4.22.2.1	Use case - Broadcast data services.....	72
4.22.2.2	Use case - Mobile TV related services.....	72
4.22.3	Requirement for multicast dataflow (subscription and dataflow reception).....	72
4.22.4	Interaction with existing features (informative).....	72
4.23	New type of data storage and access.....	73
4.23.1	Abstract (informative).....	73
4.23.2	Background (informative).....	73
4.23.2.0	General.....	73
4.23.2.1	Use case - Taking a picture from the terminal, storing it on the UICC and retrieving it.....	73
4.23.2.2	Use case - Storing and protecting data through operator portal.....	73
4.23.2.3	Use case - Storing a service description.....	73
4.23.2.4	Use case - Managing multimedia content via UICC to a remote server.....	73
4.23.2.5	Use case - Partitioning UICC memory.....	74
4.23.2.6	Use case - UICC content depending on user authentication.....	74
4.23.2.7	Use case - Migration to a USB UICC without ICCD class.....	74
4.23.3	Requirements.....	74
4.23.3.1	Data storage and structure requirements.....	74
4.23.3.2	Data protection requirements.....	75
4.23.3.3	Local and remote access requirements.....	75
4.23.4	Interaction with existing features (informative).....	75
4.24	CAT access over a modem interface.....	75
4.24.1	Abstract (informative).....	75
4.24.2	Background (informative).....	76
4.24.2.0	General.....	76
4.24.2.1	Use case - Extending CAT to the connected entity capabilities.....	76
4.24.2.2	Use case - Using CAT for data acquisition and control in an M2M device.....	76
4.24.2.3	Use case - Addition of CAT support by adding a CAT extender device.....	77
4.24.3	Requirements.....	77
4.24.3.1	General requirements.....	77
4.24.3.2	Connected device registration requirements.....	78
4.24.3.3	Legacy support requirements.....	78
4.24.3.4	Extended support requirements.....	80
4.24.3.5	CAT over modem-client interface requirements.....	80
4.24.3.6	Connected entity termination requirements.....	80
4.24.3.7	Security requirements.....	81
4.24.4	Interaction with existing features (informative).....	81
4.25	UICC-Terminal applications and services over USB.....	81
4.25.1	Abstract (informative).....	81
4.25.2	Background (informative).....	81
4.25.2.1	Use case - Migration of existing services over IP.....	81

4.25.2.2	Use case - End-user interaction.....	82
4.25.2.3	Use case - Integration of UICC services into terminal user interface	82
4.25.2.4	Use case - Access status of communication services	82
4.25.2.5	Use case - Access to specific terminal hardware.....	82
4.25.2.6	Use case - Interaction between terminal and UICC applications	83
4.25.3	Requirements	83
4.25.3.1	General framework requirements.....	83
4.25.3.2	Framework service discovery and management requirements.....	83
4.25.3.3	Interaction between UICC and terminal applications requirements.....	84
4.25.3.4	Framework security requirements	84
4.25.3.5	User Interface requirements	84
4.25.3.6	Device interaction requirements.....	85
4.25.3.7	Network related requirements	85
4.25.3.8	Specific Services requirements	85
4.25.3.9	Backwards compatibility requirements.....	85
4.25.4	Interaction with existing features (informative).....	85
4.26	Integration of a UICC in a Mobile Broadband Notebook	85
4.26.1	Abstract (informative).....	85
4.26.2	Background (informative).....	86
4.26.2.1	Architecture considerations.....	86
4.26.2.2	Use cases	86
4.26.2.2.1	Authentication	86
4.26.2.2.2	Mass storage for MNO content	87
4.26.2.2.3	Mass storage for user content	87
4.26.2.2.4	Cryptographic services	87
4.26.2.2.5	Web services.....	87
4.26.2.2.6	Secure execution environment.....	88
4.26.2.2.7	Device Management	88
4.26.2.3	Security considerations	88
4.26.3	Requirements	88
4.26.3.1	Generic requirements	88
4.26.3.2	Security requirements.....	89
4.26.3.3	Security policy related requirements.....	89
4.26.4	Interaction with existing features (informative).....	89
4.27	Fourth UICC Form Factor	89
4.27.1	Abstract (informative).....	89
4.27.2	Background (informative).....	89
4.27.2.0	General	89
4.27.2.1	Use Case - Introduction of new devices that can support UICC	89
4.27.2.2	Use Case - Slimmer mobile devices.....	89
4.27.2.3	Use Case - Enhanced end user experience	90
4.27.3	Technical Solution Selection Criteria	90
4.27.4	Requirements	90
Annex A (informative):	Requirement numbering scheme.....	91
Annex B (informative):	Change history	92
History		94

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Smart Card Platform (SCP).

The contents of the present document are subject to continuing work within TC SCP and may change following formal TC SCP approval. If TC SCP modifies the contents of the present document, it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 0 early working draft;
 - 1 presented to TC SCP for information;
 - 2 presented to TC SCP for approval;
 - 3 or greater indicates TC SCP approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document specifies the requirements for Release 7 onwards of the TC SCP.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/8a7ec42d-5a66-412-b830-594889e8289b/etsi-ts-102-412-v11.2.0-2019-06>

1 Scope

The present document specifies the additional requirements for Release 7 onwards of the TC SCP with respect to earlier releases.

The present document covers all the Stage 1 requirements which are not covered by other TC SCP stage 1 documents.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- In the case of a reference to a TC SCP document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

Referenced documents which are not found to be publicly available in the expected location might be found at <https://docbox.etsi.org/Reference/>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

- [1] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 7)".
- [2] ETSI TS 102 223: "Smart cards; Card Application Toolkit (CAT) (Release 6)".
- [3] ETSI TS 122 038: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); USIM Application Toolkit (USAT/SAT); Service description; Stage 1 (3GPP TS 22.038 Release 7)".
- [4] ETSI TS 151 011: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (3GPP TS 51.011)".
- [5] ETSI TS 131 102: "Universal Mobile Telecommunications System (UMTS); LTE; Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102 Release 6)".
- [6] ISO/IEC 7816-4: "Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange".
- [7] Trusted Computing Group (2003): "TPM Main - Part 1 Design Principles - Specification version 1.2".
- [8] ISO/IEC 14443 (all parts): "Cards and security devices for personal identification -- Contactless proximity objects".
- [9] ISO/IEC 18092: "Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1)".
- [10] ISO/IEC 15693 (all parts): "Cards and security devices for personal identification -- Contactless vicinity objects".
- [11] ETSI EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".
- [12] ETSI EN 302 304: "Digital Video Broadcasting (DVB); Transmission System for Handheld Terminals (DVB-H)".

- [13] OMA-TS-SRM-V1_0-20090310-A: "OMA Secure Removable Media Specification".
- [14] OMA-AD-SRM-V1_0-0-20090310-A: "OMA Secure Removable Media Architecture".
- [15] OMA-RD-SRM-V1_0-20090310-A: "OMA Secure Removable Media Requirements".
- [16] ETSI TS 102 241: "Smart Cards; UICC Application Programming Interface (UICC API) for Java Card (TM) (Release 8)".
- [17] ETSI TS 127 007: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; AT command set for User Equipment (UE) (3GPP TS 27.007 Release 9)".
- [18] ETSI TS 102 613: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics".
- [19] ETSI TS 102 622: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI)".
- [20] ISO/IEC 18000 (all parts): "Information technology -- Radio frequency identification for item management".
- [21] ETSI TS 102 483: "Smart cards; UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal (Release 8)".
- [22] IETF RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1".
- NOTE: Obsoleted by IETF RFC 7230, IETF RFC 7231, IETF RFC 7232, IETF RFC 7233, IETF RFC 7234 and IETF RFC 7235.
- [23] ETSI TS 102 484: "Smart Cards; Secure channel between a UICC and an end-point terminal".
- [24] ETSI TS 102 600: "Smart Cards; UICC-Terminal interface; Characteristics of the USB interface".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- In the case of a reference to a TC SCP document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] GSMA Pay Buy Mobile, Business Opportunity Analysis, Public White Paper, version 1.0, November 2007.
- [i.2] ISO/IEC 16750-3: "Road vehicles -- Environmental conditions and testing for electrical and electronic equipment -- Part 3: Mechanical loads".
- [i.3] AEC-Q100: "Stress Test Qualification for Integrated Circuits".
- [i.4] OMA-TS-BCAST-SvcCntProtection-V1.0: "Service and Content Protection for Mobile Broadcast Services".
- [i.5] Mobile Broadband in Notebooks Guidelines, version 4.0, December 2009.
- [i.6] ETSI TR 102 906: "Smart Cards; UICC-Terminal interface; UICC in Mobile Broadband Notebook".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

4FF: Fourth UICC form factor

AT command interface: modem interface protocol specified in ETSI TS 127 007 [17]

card emulation mode: mode of operation where the UICC emulates a contactless card through the CLF

central repository: repository of registered applications residing in the UICC

chunked transfer-coding: mechanism that allows HTTP messages to be split in several parts as defined in IETF RFC 2616 [22]

CLFI (CLF Interface): physical interface between the UICC and the CLF

CLFIP (CLFI Protocol): communication protocol between the UICC and the CLF carried over the CLFI

ContactLess Front-end (CLF): circuitry in the terminal which:

- Handles the analog part of the contactless communication.
- May handle some layers of the contactless protocol.
- May exchange data with the terminal and the UICC.

DRM Agent: entity in the Device that manages Permissions for Media Objects on the Device, as described in OMA SRM technical specification [13]

DRM Agent-SRM Agent Mutual Authentication: DRM Agent and the SRM Agent can authenticate each other based on credentials that are securely provisioned in each

NOTE: The result of this mutual authentication allows the DRM Agent and SRM Agent to establish a secure communication for the exchange and sharing of secret elements as described in the OMA SRM architecture specification [14].

external entity: entity that is external to the UICC and the modem; it can be the Mobile Broadband Notebook or a distant entity (e.g. a server)

High Speed Protocol (HSP): running on top of the NUT interface

Host Controller Interface (HCI): HCI is a part of the implementation of CLFIP, as defined in ETSI TS 102 622 [19]

M2M communication module: electronics system including all necessary components to establish wireless communications between machines

NOTE: M2M communication modules are usually integrated directly into target devices, such as Automated Meter Readers (AMRs), vending machines, alarm systems, cars equipment's or others.

M2M device applications: applications deployed on a machine to machine device that deliver a service to the UICC

M2M UICC: UICC with specific properties for use in M2M environments, this includes existing form factors and an optional new form factor

Machine to Machine (Communication): communication between remotely deployed devices with specific responsibilities and requiring little or no human intervention, which are all connected to a dedicated management server via the mobile network data communications

ME/TE owner: entity having the right to configure or administrate a CAD and/or remote terminal

MFF (M2M Form Factor): new form factor dedicated to M2M applications